GlobalLogic®

Blockchain Interoperability (Part 1)

By
Harish Jaggi & Raj Jha

Abstract

This paper describes interoperability, challenges in achieving it, possible solutions, their evolution and author recommendations based on research done during the last four months. Lack of interoperability and scalability are huge challenges to the true potential of blockchain technology. This paper provides a guide for selecting the right solution in various use cases and problem statements. Critical levers have been compared among top solutions, and examples of pertinent use cases are mapped to each solution, thereby making the conclusion derived from both quantitative and qualitative perspectives. Comparisons are drawn based on a comprehensive set of factors consisting of token portability, atomic swap, cross-chain Oracle, asset encumbrance, interoperability, data exchange, third-party need, security, latency, vulnerability, ease of implementation, transaction finality, consensus protocols, maintenance and scalability. Interoperability, regulatory challenges and scalability are the biggest challenges to the success of blockchain technology.

Our research infuses optimism and enthusiasm about the future of blockchain technology with credible solutions to interoperability, scalability and regulatory challenges that are ready for production. In-depth analysis of interoperability is the prime focus of this paper, and our research on scalability and regulatory challenges will be discussed in another paper, as these are equally important and complex topics. The biggest advantage of this paper is that architects can instantly select the right interoperability solution pertaining to side-chain, Notary, hashed-time-lock, Oracle, API Gateway, co-chains, and engines based on the business problem at hand.

Contents

Background

Blockchain stature is growing with each passing day. As an offshoot of its growing impact, its network and corresponding chains are spreading exponentially. During the last few years, there have been several successful blockchain solutions in production around the globe that have added significant value in enterprise solutions. Though these solutions are of immense use, interconnecting the growing number of disparate chains will further help widen the horizon of its application in an exponential way. The solution to interoperability will be the eureka moment and a shot in the arm. As proponents of blockchain technology, we are very excited to witness history in the making.

The Broader Concept of Interoperability

The operation of chains in isolation has curtailed the full benefits of blockchain technology. This is because diverse blockchains are unable to communicate with one another to exchange data. In end-to-end enterprise solutions, decentralization can be achieved partially with a traditional approach. The solution to this problem statement is known as interoperability. With interoperability among various chains, information sharing will become realistic and the paradigm of blockchain solutions will travel miles ahead. This will allow end-to-end communication for all systems, including diverse chains, thereby realizing the full potential of decentralization. Interoperability will break all boundaries in such a blockchain solution, making it reap its true potential. Some of the use cases after interoperability solutions become seamless are:

1. Diverse hospital chains running on individual chains can exchange patient data information to share medical records. This will save precious lives, as surgeries can be done by relying on another chain's findings.
2. Various states in a country can exchange vehicle data to ensure compliance.
3. Partner applications that are part of a consortium can exchange critical transaction data.
4. Cryptocurrencies can be exchanged.
5. Royalties for partners and intermediaries can be paid instantly, based on smart contracts' transaction exchange.
6. Disputes can be addressed instantly.
7. A truly digital economy can be achieved, thereby shattering the parallel grey market.
8. Hybrid blockchain will become immensely useful as public and private blockchains get to work under one umbrella.
9. Standardization will go up significantly.
10. The cost of the end-to-end solution will go down.

The possibilities are endless and this is just the tip of the iceberg.

Why Businesses Need Interoperability

With blockchain being a nascent technology, every blockchain platform's frameworks and business solutions are being worked on in silos using different mechanisms for governance, data modelling, consensus, technical stack, on-boarding, auth architecture, smart-contract architecture and infrastructure models. Due to a lack of clarity around data standards and governance, businesses do not want to invest in ambiguous solutions. There are concerns around the entry barrier and changing costs if things go south. Businesses need the flexibility to switch solutions with ease and interoperate with other systems, rather than reinvent the wheel and add huge costs.

In a scenario where industry/consortium/business "A" with their blockchain solution intends to do business with industry/consortium/business "B" with its own dedicated yet disparate blockchain solution in place, interoperability becomes essential for a handshake and data exchange.

In a different scenario where a business needs to have different types of blockchains co-existing to perform different operations (known as a hybrid blockchain model), interoperability has an immense role to play.

There are many more applications for interoperability that will revolutionize the blockchain industry.

Interoperability Study - WEF Report

The most impactful paper on interoperability has recently come from the World Economic Forum. Snippets from the paper are as follows:

"Like the early days of the Internet when private Intranets dominated the scene, blockchain is balkanized in silos. Efforts such as those by Cosmos or the partnership between Ethereum and Hyperledger may enable an interoperable Internet of blockchains."

"While some platforms like Ripple claim they're ready for visa-level volume, most platforms have much to do to scale their solutions. Ethereum, a dominant platform for smart contracts and application development, can still process only 15 transactions per second, and its Istanbul upgrade faced numerous delays. Interoperability is likely to alleviate this problem as users marshal multiple blockchains to achieve scale."

Interoperability is a key challenge to address after the COVID-19 pandemic is over. This is not only a technology problem, but it also spans diverse views of business models, war among tech giants, governance and data ownership.

Fundamental Challenges to Interoperability

In this heterogeneous blockchain environment, interoperability enables blockchains to communicate and exchange data amongst diverse chains. Blockchain interoperability is not as simple as the integration of systems using APIs, due to the following reasons:

1. Blockchain does not allow updates or deletion of records.

2. To achieve interoperability, transactions have to be atomic on both blockchains (i.e., if Harish transfers an asset from blockchain X to Raj on blockchain Y, either Harish is debited and Raj gets credited, or neither action takes place).

3. Different blockchains are using different finality mechanisms (based on the consensus they use), hence the transaction inputs must be final from blockchain X to blockchain Y as a prerequisite.

4. Each blockchain is solving a specific problem and hence driving operations in silos for data and values.

5. Lack of data, governance and cross-chain protocol standards are a big hindrance. Data, identity and events are recorded differently on each blockchain, making data exchange complex.

6. Regulatory constraints: A few regulatory bodies across the world have not yet approved blockchain cryptocurrencies and operations.

7. Diverse blockchain topologies (public, private, hybrid) make the situation even more obscure.

8. Diverse underneath technologies: Smart contract and SDK technologies vary in different blockchain platforms, which is another big problem that needs to be addressed.

These challenges are some of the hindrances to achieving interoperability.

Our Research on Interoperability

Interoperability among blockchains has been a work in progress for a few years now, but industrial case studies are rare. Our findings are based on meticulous research of every single solution offered under the sun.

Initially, interoperability of blockchain research revolved around "cryptos" due to the lack of permissioned blockchain in the industry. The criteria to classify interoperability was typically based on "Buterin's Classification," i.e., side-chain (also known as relay chain), Notary schemes and timed hash locks.

Side-Chain

Two existing blockchains (BA, BB) can interoperate and scale (shard) using side-chain mechanisms where BA is main-chain and BB is extension blockchain for BA (a side-chain). The main characteristics of side-chain mechanisms are:

1. Main-chain maintains a ledger of assets.

2. Communication between main-chain and side-chain happens using cross-chain communication protocol, tightly coupled with functions of both the blockchains.

3. In the above case, any blockchain (BA or BB) can become a side-chain to the other.

4. The most common example of transfer of assets between the main-chain and the side-chain is a two-way peg. In a two-way peg, a user aligned on the main-chain percolates crypto tokens to a special address. Funds are locked on the main-chain while a corresponding number of tokens are replicated on the side-chain. Players, users or entities can use the tokens on the side-chain. That being said, the users can send the tokens back to the main-chain, which then turns assets on the side-chain into a locked/destroyed state, based on the scenario signed between the entities.

Here are three prominent Ethereum and bitcoin side-chain implementations.

Side-chain	Main-chain	Side-chain Consensus
Loom Network	Ethereum	Delegated Proof of Stake
Liquid	Bitcoin	Strong Federations
BTC Network	Ethereum	N.A.

Note: Explaining the consensus mechanisms used by side-chains is beyond the scope of this paper.

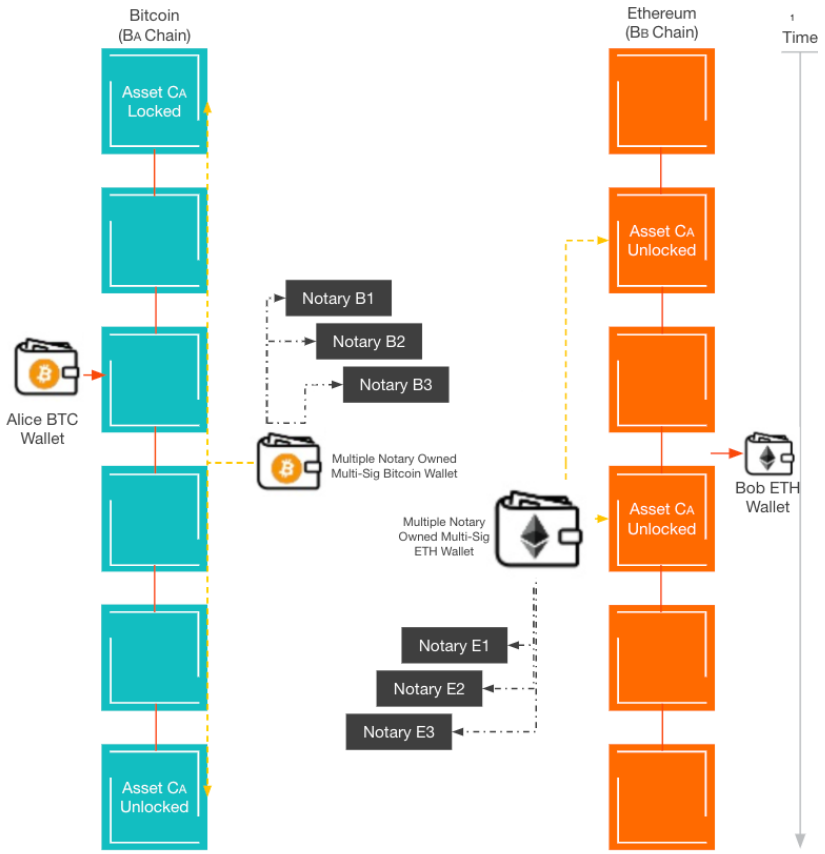
Notary Scheme

Notary is a credible mechanism to prove triggered transactions on a blockchain after an event occurs on another blockchain. Notary schemes can have varied degrees of decentralization when more than one notary is employed. Notary schemes simplify the task of cross-chain transactions. Contrary to side-chains, Notary schemes are not extensions of a blockchain. Rather, they are often centralized third parties (e.g., centralized crypto exchanges).

Binance and coinbase crypto exchange platforms are examples of a centralized (single) Notary. Ripple is also using Notary mechanisms to exchange assets between global financial companies. Polkadot and interledger platform mechanisms fall under a decentralized Notary scheme (due to validators associated with each parachain).

We will describe the Polkadot mechanism in detail under the "Engine" section, as it also qualifies as an interoperability engine. The overall Polkadot network is perceived as a single unified state machine that renders complete blockchain-to-blockchain APIs. This results in easier upgrade processes and equips member chains with a layer of solid shared security.

Suppose a user named Alice intends to transfer the native crypto asset CA of blockchain BA on blockchain BB. Alice will lock the asset of blockchain BA to a multisig wallet attached to blockchain BA and owned by a set of reputable and trusted notaries running on a full node. Once this is completed, a second multisig wallet owned by a set of reputable notaries and attached to blockchain BB will unlock asset CA on blockchain BB. If an asset can be accepted from chain BB to chain BA and vice versa, the system becomes two-way pegged.



Hashed-Time-Lock

Hashed-time-lock contracts enable cross-chain atomic operations and use hash-locks and time-locks (locking for a period of time to guess the plain text of a cryptographic proof hash). These techniques carry out payments, normally between two parties.

Atomic swaps are a subset of the hashed-time-lock contract techniques, enabling cross-chain exchanges. Atomic swaps allow a user to send a certain amount of crypto assets to another user in exchange for another crypto asset held on another blockchain.

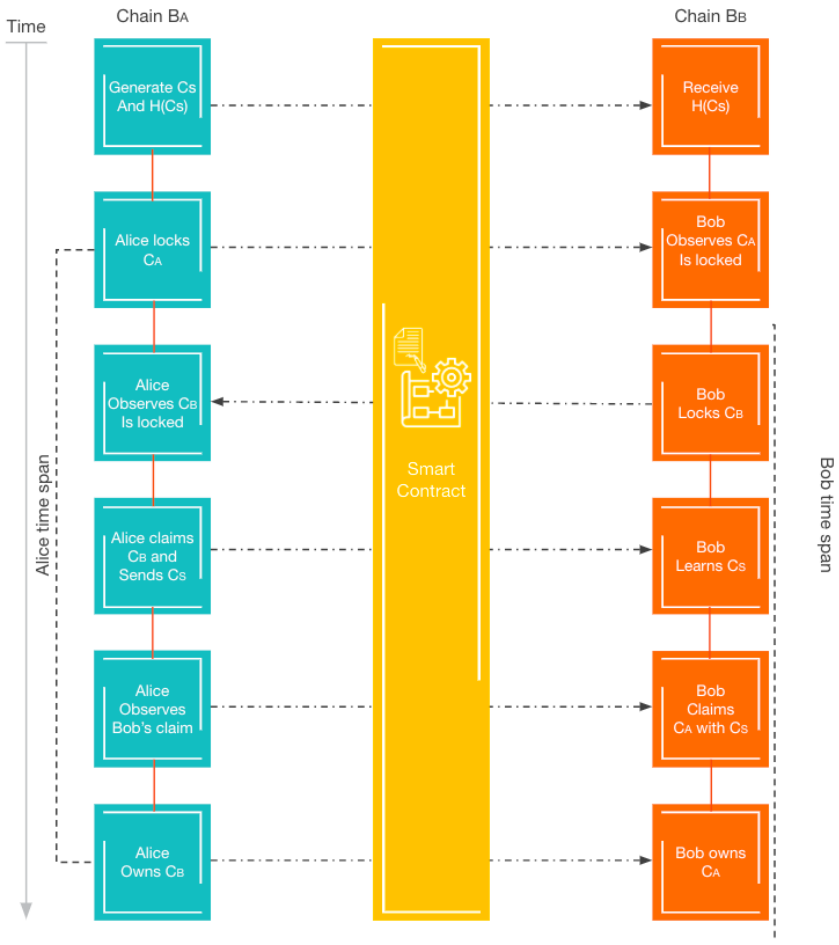
For example, Alice wants to exchange an asset CA on blockchain BA with Bob, whose asset CB is on blockchain BB.

At the onset, Alice generates a cryptographic secret Cs and sends the secret's hash H(Cs) to Bob. In step 2, Alice locks her asset in a smart contract.

Bob then observes that asset CA is now locked in the smart contract and he locks his asset CB in the same contract. Alice sends a transaction to claim asset CB along with secret Cs.

As Bob knows the secret, he is now in a position to unlock asset CA and take possession seamlessly.

If any issue occurs during asset transmission or receipt, assets are unlocked and given back to respective owners after a predefined time configured in the exchange.



Wanchain is an apt solution that belongs to hashed-time-locks. It focuses mainly on offering deposit and loan services via cryptocurrencies. This has evolved a lot in the last few years. After accepting a transfer request, it issues an appropriate number of tokens through a smart contract that in turn escrows them on the target blockchain. Thereafter, its validator nodes receive a request, and upon verification of the transaction occurrence, it creates an impersonation of the tokens to be transferred to the destination blockchain.

An important consideration to add is that Buterin's classification is mainly based on a crypto approach and mostly limited to permissionless blockchains.

Blockchain Interoperability - Part 2:

This is not the complete picture. There is more content based on the research we have undertaken. Read Part 2 of the whitepaper to get deeper insights. In the second part, we have analyzed a few more interoperability criteria such as Oracle, API gateways and co-chain-based models for hybrid blockchain, published research-oriented quantitative results and collated recommendations on business applicability.

About the Authors

Harish Jaggi is a hard-core techie, a researcher, blockchain incubation expert, and a huge proponent of blockchain technology. He is spearheading the India charter of blockchain practice at Globallogic. He has over 20 years of extensive experience in the Information Technology industry and has 12 diverse certifications, including 3 on blockchain technology. He has extensively worked on Ethereum, Hyperledger, Solidity and Interoperability research in diverse domains. He has spearheaded blockchain projects, advisories, and initiatives since 2015. He is a regular speaker in prominent forums and meetups on blockchain technology. Many of his articles have been published by leading media houses.

Raj Jha is a researcher, open-source contributor and blockchain architect with several successful blockchain implementations to his credit. He is a senior blockchain architect at Globallogic. He carries 15 years of diverse experience in the Information Technology industry. He carries many certifications, including blockchain solution architect certification. He has extensively worked on Ethereum, Hyperledger, Solidity and Interoperability research in niche areas of application. He has played a coveted role in blockchain projects, advisories, and initiatives for years. His expertise lies in the integration of blockchain with third parties and prominent tools. Many of his articles have been published by leading media houses.

GlobalLogic®

GlobalLogic is a leader in digital product engineering. We help our clients design and build innovative products, platforms, and digital experiences for the modern world. By integrating strategic design, complex engineering, and vertical industry expertise, we help our clients imagine what's possible and accelerate their transition into tomorrow's digital businesses. Headquartered in Silicon Valley, GlobalLogic operates design studios and engineering centers around the world, extending our deep expertise to customers in the communications, automotive, healthcare, technology, media and entertainment, manufacturing, and semiconductor industries.



www.globallogic.com